International Annals of Science
ISSN: 2456-7132
Volume 8, Issue 1, pp. 30-37, 2020
DOI: https://doi.org/10.21467/ias.8.1.30-37

SHORT REVIEW

# Survey on Security for WSN based VANET using ECC

Kalkundri Ravi[1*], Rajashri Khanai[2+], Kalkundri Praveen[2]

[1] Dept. of Computer Science and Engineering, K.L.S's Gogte Institute of Technology
[2] Dept. of Electronic &Communication, KLE Society's College of Engineering & Technology

* Corresponding author email: ravi.kalkundri05@gmail.com

Received: 14 March 2019 / Revised: 25 June 2019 / Accepted: 06 July 2019 / Published: 22 July 2019

## ABSTRACT

With the increase in population, there is an increase in the number of car users drastically. Around the world, either millions of people die due to car accidents or they are severely injured by the accident. Most of the accidents occur due to lack of common information the drivers, as the lane change, applying sudden break, traffic congestion, etc, are the causes of accidents. Safety information such as speed limits, road conditions, traffic status, accidents, etc..., are used in some countries, but still more work is to be achieved. Vehicular Ad Hoc Networks (VANET) should be implemented and they should collect and distribute necessary safety information to other vehicles. VANET is a combination of Road Side Units (RSU's) and On-Board Units (OBU's). These RSU's and OBU's consist of various sensors, which are used to collect various data. The data collected by the sensors on the OBU's on the vehicles can either be sent to another vehicle or can be displayed to the driver. Similarly, the sensor collects data at the RSU and sends the data to other RSU or depending on its nature and importance, the RSU may even be broadcasted to other vehicles. The main objective is to provide safety to the drivers, the passengers and to the information that is being transmitted between the nodes. However, in some scenarios, VANET's may not guarantee timely detection of issues or any type of dangerous. We propose a solution by the integration of VANET and WSN to create a hybrid infrastructure with the in inexpensive wireless sensor nodes integrated on RSU's along the roadside and on the OBU's in the vehicle. As the new hybrid structure is proposed, there may be challenges that may occur. This article discussed these challenges and solutions to create an efficient and well-organized VANET-WSN Hybrid network.

**Keyword:** Security, VANET, WSN.

## 1 Introduction

Vehicular Ad Hoc Networks (VANETs) technology is a recent generation wireless networks, which are part of MANET's applied to vehicles. VANETs comprises of different ad hoc networks, formed using of short-range radio and long-range radio in vehicles. Therefore, VANETs are required to be equipped with short-range and long-range radios for communication. Communication in the networks involve both Vehicle-to-Vehicle (V–V) and Vehicle-to-Infrastructure (V–I) communications, as seen in Figure 1. Vehicles communicate with one another or with the infrastructure when they are within

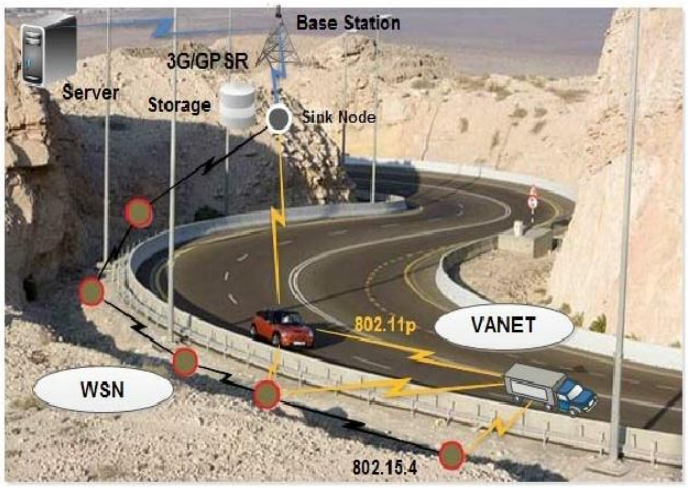


**Figure 1:** *A VANET-WSN scenario (courtesy [3]).*

their transmission ranges. The roadside infrastructure is wide spread and the layout depends upon the region and if required the infrastructure can be extended for better deployment. The overall network works with the technique that the vehicles communicate with other vehicle or with infrastructure only when they are in the range or the communication takes place at regular intervals. The infrastructure or RSU has is installed along the roadside or at the intersections. These RSU's provide information to the vehicles like, information on safety, , road status, traffic conditions and infotainment, and information from central authority station [1][2]. Applying Wireless sensor for VANET's have provides significant advantages in terms of cost and distribution of data. The cost of installation and maintenance are reduced, but WSN cannot be used as a standalone system, it need some additional components and works as a heterogeneous system and collaborates with other technologies. WSN systems have some limitations such as in processing and with energy resources etc. [1]. On the other hand, VANETs has several challenges, such as VANET's are large-scale infrastructure and are extremely mobile network. Vehicles or nodes are dynamic in nature in the VANET environment, as the speed of all the cars is not same and their locations are constantly changing. The high mobility in the vehicles leads to change in network topology dynamically. This leads link to break and connect when the vehicles are in range, i.e. nodes connect when they are in range and disconnect when they are out of range very often. Besides, VANETs have a potentially large scale which various types of messages to share among the vehicles or the RSU. Other information are like the traffic flow, congestion, accidents, routs, etc., are also maintained by the VANET and the infrastructure. In VANET, the communication takes place between Vehicle-to-Vehicle and Vehicle-to-Road Side Unit (RSU). WSN based applications are interesting and best alternate because of low suitable for VANET. Some of the most relevant applications and their functions show in Figure 1 [4].

### 1.1 VANET Advantages

VANET helps to improve the road safety by providing information or warning to the drivers if any road accidents occur ahead or if there is a congestion or roadblock. This helps the driving experience and also provides more information for the drivers during the journey. VANETs also provide vital information like vehicle owner, tracking the vehicle at times of trouble, like accident, theft, etc., to the central authorities and management. Further VANETs also provide other useful applications like payments at various places like tolls, petrol pumps, servicing stations, etc. VANET networks are self-sustained, which means that if any node or vehicle fails, it does not affect the entire networks performance. VANETs are Self-configuring nodes and Self-healing network. VANETs are separate from central network administration as the nodes are independent in nature; rather they form clusters of nodes. VANETs are a vast and huge network and are scalable to any number of nodes, which can add or remove any number of nodes dynamically. The nodes in the network connected and communicated quickly irrespective of any hardware and software.

Like any network, VANET's also have come some challenges, which have to be addressed. Some of the challenges are that VANET's have a large, bulk-sized network; this also can be a problem some times. Since the nodes travel at various speeds, the nodes are at high mobile and dynamically change their topology, resulting in unstable connection between cars/nodes. Due to the above two reasons, providing security is also a major issue. Further issues also arise in key distribution in VANET, preserving user privacy, secure communication between nodes, etc. All the above issues, researchers are encouraged to study and find a suitable solution for VANET's.

### 1.2 Security Requirements in VANETs

Since VANET network is open in nature, the data transmission is also vulnerable to any kind of attacks. Thus, VANET's also require some sort of security features. Providing security to VANET satisfies the subsequent requirements [6][7].

***Authentication:*** Authentication makes sure that the intended sender has sent the message and receiver is an intended receiver. In VANET, a vehicle collects information from the neighbouring nodes or from the nodes that are coming from the opposite direction.

***Accessibility*:** This affirms that only the intended sender and receiver should be accessing the data. If any attack takes place, the system must be able to handle the attack or it should close the system or terminate the connection, in order to protect the data. VANET works with the goal of sharing data only to the intended user.

***Information verification*:** Any false or malicious information, VANET should be able to handle such messages that are received. The network must kill those false messaging or tackle the messages.

***Privacy*:** Privacy must be maintained between the authenticated used and should be avoided from unauthorised users.

***Emergency information*:** If any accidents occur in two or more vehicles, information regarding the vehicles in the emergency must be recorded and a message is to be broadcasted to other vehicles, which are in the same path.

***Tamper evidence hardware*:** To protect the information from leakage and to keep the information safer, tamper proof system should be maintained.

***Reliability*:** One of the basic requirements is reliability of users, which ensures that the message is delivered to the destination and a reliable transmission of messages.

***Scalability*:** Here scalability refers to how network can handle the dynamic mobile nodes scalable networks i.e., the network must be capable to handle if nodes increase or decrease drastically and should not degrade the performance of network.

## 1.3 Types of VANET Attacks

There are various types of attacks for VANET's, based on the security requirements, they are shown below [5][6][7]:

### 1.3.1 Attacks on Availability

***Denial-of-Service:*** This type of attacks handles if any duplicate messages are sent to the receiver or to the Road Side Units (RSU) to cause unwanted trouble in the communication in the VANET infrastructure.

***Jamming:*** This attack is similar to DoS attack, but this attack just jams the communication by inserting false dummy information or disabling the RSUs or intermediate nodes.

***Broadcast tampering:*** In this type of attack, unauthorised node/person will broadcast false information, which may cause large problems in VANET.

***Malware:*** An attacker will update some false information into the VANET services. Insider attackers execute these attacks.

***Spamming:*** Here in this type of attack, the attacker will flood repeated or garbage packets, which may reduce the overall performance of VANET.

***Black hole attack:*** In this attack, the malicious nodes deny or refuse to receive packets resulting in data packet loss in VANET.

### 1.3.2 Attacks on Authenticity

***Sybil attack:*** In this attack, the malicious node pretends as if they are numerous nodes.

***Replay attack:*** Here, the attacker intercepts the data or information, and further creates duplicate copies of the message and inserts into the network, creating extra burden in the network.

***Position faking and GPS spoofing:*** In this type of attack, the location of the nodes is manipulated to create various troubles in the VANET network.

***Tunnelling:*** The attacker establishes a private connection, which is identical to wormhole attack using the same network infrastructure.

***Key/certificate replication:*** To increase the confusion, the attacker replicates or generates malicious secret security key or certificate, which creates delay in the transmission.

***Message tampering or alteration:*** Here the attacker tries to change, modify or delete some part of the message or the entire message, creating the issues between the nodes.

### 1.3.3 Attacks on Confidentiality

***Eavesdropping attack:*** Here, the attacker listeners to the transmission channel between the intended nodes. Once the attacker acquires the

information, he utilises the information to attack the nodes or the entire system. The attack allows the attacker to collect various information, such as node location data, message timing, duration, message size, etc...

***Traffic analysis attack:*** Here the attacker analyses the type of the nodes in the network and tries to employ some means of method to create disturbance in the network. The attacker also tries to study the types of nodes that are part of the network.

### 1.3.4 Attacks on Integrity

***Masquerading:*** Here the attacker tries to impersonate as some other vehicles or node by providing false ID, false security key, etc... This further leads to attacks like man-in-middle attack and authenticity.

### 1.3.5 Other attacks

***Bogus information attack:*** The attacker sends false or dummy information to other nodes for their benefits or just to create any sort of issues in the network.

***Malicious node attack:*** Here the node intentionally or unintentionally misbehaves in the network, creating issues between the communicating nodes. Further, the nodes misbehave during the communication, such as they introduce delay in communication, due to high-speed lag in responding at the proper time and so on.

***Selective forwarding:*** Here the attacker deliberately changes the course of the packets travelling in the network.

***Flooding of RREQ message:*** This type of attack is concerned with the reply request messages to be flooded in the network. This leads to excess messages, killing or delaying the current or the most recent messages.

## 2 Overview of VANET-WSN System

WSN's have some features such, as they are less costly, they consume low power, can communicate in short-range or long-range wirelessly, fast and instant data processing and data transfer. These advantages of WSN encourage us to integrate WSN into the VANET infrastructure. WSN's can provide timely detection of road conditions; provide vital information, multimedia data, etc... Sensors used in roadside stations of current VANETs system are expensive than wireless sensor nodes which are too cheap [7]. Further, WSN's consumes low power, they are smaller and have small-size sensing modules and can be installed anywhere on the RSU's to gather road conditions, traffic analysis, data transfer, etc...Such sensor nodes along with the RSU's can be deployed along the roadside, where such RSU's group form a cluster and all together connect to the base station so as to work together with the VANET. Mover over these sensor nodes also stores safety-related information generated by the vehicles in the infrastructure, and further forward the information to other vehicles in different partitions of the VANET infrastructure [7].

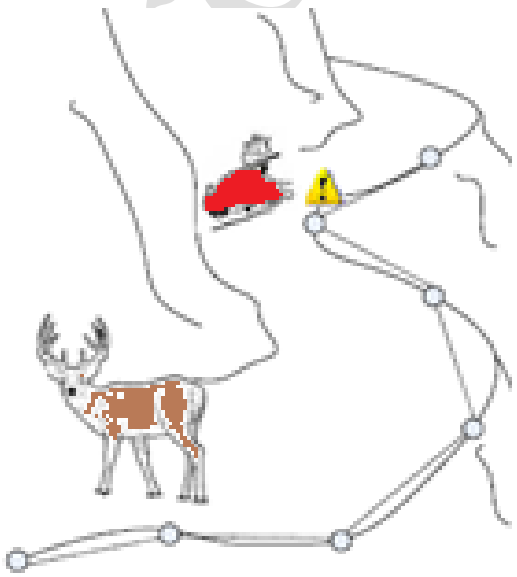

**Figure 2:** *A VANET-WSN Hybrid System.*

Figure 2 explains a VANET-WSN Hybrid System based application. The above figure 2 is an example in where a WSN based node is deployed to detect wildlife animal on the mountainary roadway, as it is very difficiult to find the presence of any animal on such roads, it is also difficult during the night times ti detect the animals. The nodes detect the movement and send the message to the upcoming vehicles and also interacts within VANETinfrastructure to increase the safety of both driver's and

passenger's to avoidany accidentts and insuries to the animals [7].

## 3 Proposed Scheme

### 3.1 Proposed VANET-WSN Hybrid System

Both VANETs and WSNs have similar characteristics, such as both the networks are self-organized and self sustainable.These WSN nodes are integrated withe the RSU's that can communicate with the vehicles. Further, sensor nodes have limitations liker smaller size, limited processing capabalities and limited battery or power constraints, but the sensors have a major advantage, that they communicate via a well esatabised IEEE 802.15.4 wifi technology, and with a simple pair of AA batteries itallows any embedded systems to work for years. In cases that the nodes are at very remote location, were the maintainance for batteries is too difficult, an alternative or additional power source can be RSB (Rechargeable Solar Batteries). On the other side, the vehicles are equiped with powerful computing devices called OBUs (On Board Units), which do not have burden of more energy consumption as shown in Figure 3.

The road-side WSN-VANET hybrid communicate via the OnBoard-Unit (OBU) fitted inside the vehicles and two wireless network interfaces; namely IEEE 802.11p and IEEE 802.15.4. Once the data is collected and process if required, then the data and store the data in a distriduted and redundant database. Data is also taken from the database and transmitted to upcoming nodes or vehicles, for information such as hazard warning, multimeda, other vehicle information, traffic alearts, etc… In the proposed system, the sensor nodes are a combination of a WSN with RSU. These nodes store the collected information from the itself and other nodes, and send the data accross vehicles via IEEE 802.14. The nodes communicate with other WSN nodes by randomly partitioned into group's, also called as clusters. These cluster head are manage the nodes that are under that clusters, like a WSN Gateway. The Sensor Nodes (SNs) processes the collected data and transmit to their respective cluster heads.Further, this data is sentto other cluster heads for communication with the vehicles into the VANET which are in th range of communication. On receiving the data by the vehicle, it broadcasts the information to its neighbouring nodes or significantnodes in that region. The OBU on every vehicle plays a vital role in the VANET infrastructure, since it actsas a gateway between the WSN and the VANET.

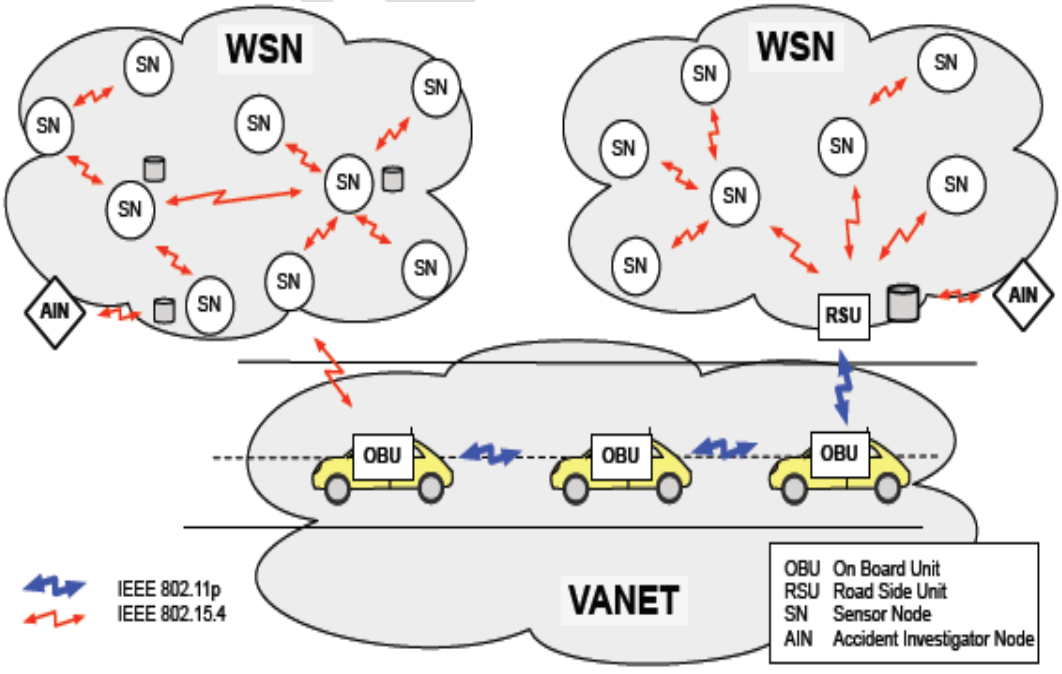


**Figure 3:***Propose VANET-WSN Hybrid System.*

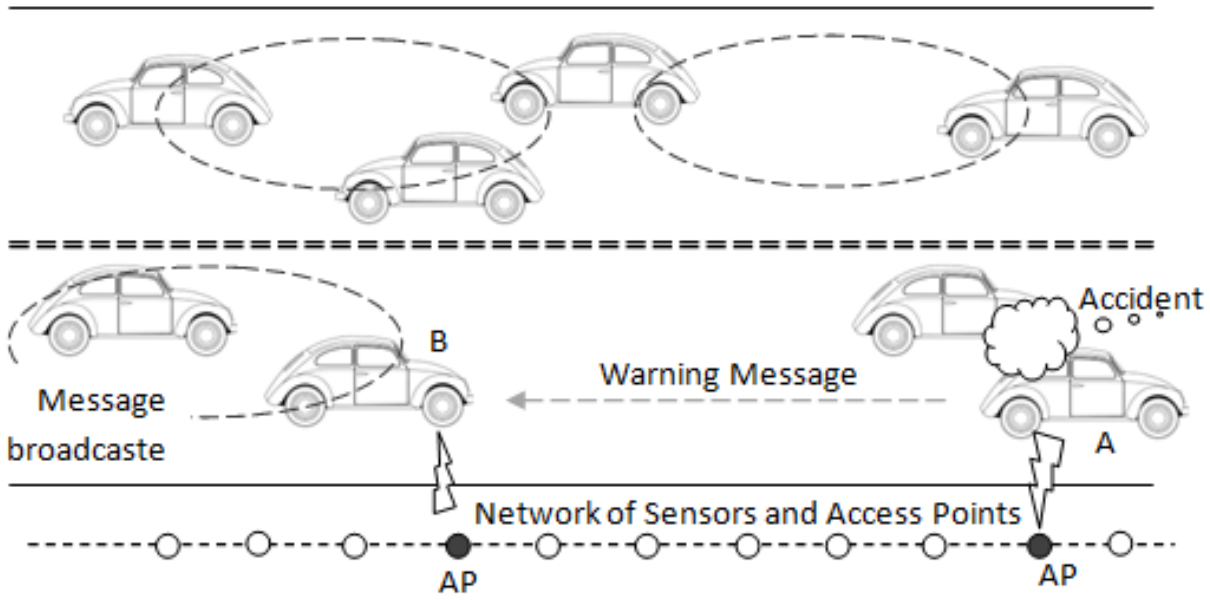


**Figure 4:** *Sensors and Access Point deployment.*

The proposed system consists of the RSU which are static roadside sensor nodes and OBU's which are highly mobile vehicle nodes. The nodes exchange data via a WiFi (IEEE 802.11) interfacewith other vehicle nodesfor data transmision; and the other method usesa ZigBee module interface (IEEE 802.15.4) with roadside sensor nodes is for transmitting data. The nodes are integrated with sensors and ZigBee interface for data transmission between sensor nodes and vehiclenodes.Figure 4 shows the deployment of sensor nodes alongthe roadside of the highway,forming a network. These sensor noces can be classified in two categories, the normal sensor node and the access point (called AP thereafter). The normal sensors can sense the acivities and transmit messages, where as the APs have additional responsibilities, like managing the vehicle network, discovering and communicating with vehicles.

APs arefew in number than theregular nodes. The nodes are formed in a specific fashion. After two regular nodes are deployed one AP node is deployed along the roadside form a group. We propose that, if three or more nodes that are connected must be an AP [7].

### 3.2 Combining P2P and VANET

Further we also propose that when vehicle to vehiccle communication has to take place, one of the most simplest way is to communicatie via the Peer-to-Peer network. The two upcoming and interesting research area in distributed computing and mobile communication domain are integrating peer-to-peer network and vehicle ad hoc network (VANET). Integrating P2P on top of VANET'sphysical infrastructure works effectively as the advantage of P2P network adds better connectivity which is very suitable for dynamic network likeVANET [8]. Large scale files like a multimedia file, or a huge text file in VANET is a challinging task. Hence implementing P2P network for file sharing shheme, as P2P nd VANET work similarly in file sharing, self oaragiseing, self sustainable to failures and distributed network. In addition, like P2P, VANET nodes are decentralized, very high mobile in nature and independent, as shown in Figure 5 below [8].

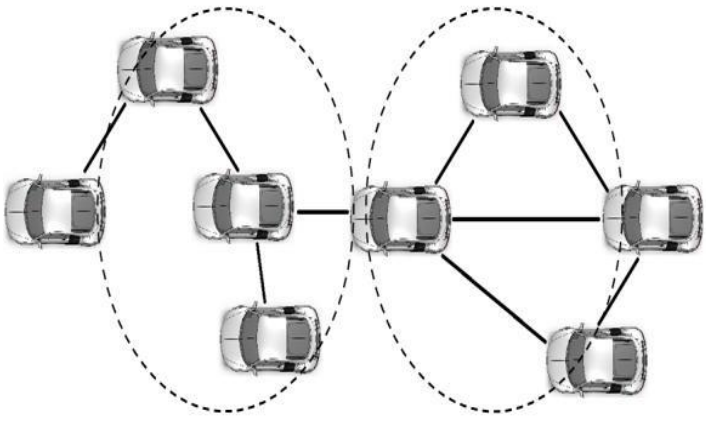

**Figure 5:** *P2P implementation onto VANET.*

Lastly, issues are also common in both P2P and vehicular networks, like frequent change in topology, as vehicles come in range and go out of range due to areas like a tunnel with no radio connectivity or the nodes are too fast to establish connection with other nodes [9][10]. P2P has varioius types of application that can be implemented on VANETs. Few applications are like online toll payment, fuel payment, video-on-demand, live streaming applications over the Internet [11]. These applications in VANET's provide a powerful platform.

### 3.3 ECC as Security for VANET

Since VANET inftastructure is open in nature, security is a major concernin information sharing through such type of networks[12].Providing security for information in the existing system, the simplest way is to use some cryptographiuc algorithm. Cryptography is an electronic technique which is used to protect valuable data, when the data is at the node or while communication.The aim of using cryptography is to protect the data which is available openly by applying some protection schemes. Cryptographic technique consists of Encryption and Decryption of data over the network. In the Encryption technique, data is converted or encrypted in an unreadable form and then sent over communication medium to the intended receiver. On the receiver side, Decryption takes place. Decryption is the reverse process of encryption, here the data is converted into readable fom [13]. There are various types of cryptographic algorithm than can be used, but only few are suitable for VANET network.

One of the upcoming cryprographic algorithm is Elliptic Curve Cryptography (ECC). ECC is one of the algorithm that is eye catching cryptosystem for mobile/wireless environments which is suitable for VANET scenatio. The advantage of ECC are like, they have smaller key size, faster computation, lower power consumption, as well as less memory and less bandwidth consumption better security level and suitable for wireless network, make ECC very suitable for VANET scenario, compared to conventional cryptosystems like RSA [14].

## 4 Conclusions

An VANET-WSN hybrid system was proposed to address the connection between the RSU's and OBU in the nodes. Further the inter commmunication between the nodes is also addressed.Hence we have proposed a VANET-WSN hybrid network for better communication. We have also suggested the use of Zigbee for better communication, where Zigbee is integrated with the RSU's. We also opropose the use of P2P model for commuication between the RSU's or within the RSU and vehivle nodes. The vechicles can communicate better by implementing P2P communication. Since VANET's communication is open, we have also addressed the various security requirements for VANET. We propose to introduce a cryptographic algorithm, to increase the security level in the VANET scenerio. We propose ECC cryptographic algorithm, which is bettter than the treditional algorithms like RSA. ECC is gaining popularities as it is suitable wireless networks, which is suitable for VANET's.

## 5 Competing Interests

The authors declared that no conflict of interest exist in this publication.

## How to Cite this Article:

Will be updated in the final version

## References


[1] Wedad Ahmed and MouradElhadef, "Securing Intelligent Vehicular Ad Hoc Networks: A Survey", J. J. Park et al. (eds.), Advances in Computer Science and Ubiquitous Computing, Lecture Notes in Electrical Engineering 474, 2018.

[2] MinSu Kim, "A Survey of Vehicular Ad-Hoc Network Security", K.J. Kim and N. Joukov (eds.), Mobile and Wireless Technologies 2017, Lecture Notes in Electrical Engineering 425, 2018.

[3] Mohammad Arif and Shish Ahmad, "Security Issues in Vehicular Ad Hoc Network: A Critical Survey", R. Singh et al. (eds.), Intelligent Communication, Control and Devices,Advances in Intelligent Systems and Computing 624, 2018.

[4] Kashif Naseer Qureshi, Abdul Hanan Abdullah and Raja Waseem Anwar,"Wireless Sensor Based Hybrid Architecture for Vehicular Ad hoc Networks", Faculty of Computing, Universiti Teknologi Malaysia, Skudai,

Johor Malaysia, TELKOMNIKA, Vol.12, No.4, December 2014, pp. 942~949.

[5] Nice Mathew and V.Uma, "VANET security -Analysis and survey", Department of Computer Science, School of Engineering and Technology, Pondicherry University, India. IEEE- International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT).-1-5386-0796-1.

[6] Rajdeep Kaur, Tejinder Pal Singh and VinayakKhajuria, "Security Issues in Vehicular Ad-hoc Network(VANET)", Department of Computer Science and Engineering, Chandigarh University, Mohali, India. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018) IEEE Conference Record: # 42666; IEEE Xplore ISBN: 978-1-5386-3570-4.

[7] Amrish Kumar and Shri Niwashn Sir, "Implementation of VANET in Transportation using Wireless Sensors", Computer Science & Engineering Subharti Institute of Engineering & Technology, Meerut, India. International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882, Volume 4, Issue 6, June 2015.

[8] Kalkundri Ravi and Dr. S.A Kulkarni, "A Secure Message Authentication Scheme for VANET using ECDSA",Department of Computer Science, K.L.S. Gogte Institute of Technology, Belgaum, Karnataka, India. 4th ICCCNT – 2013 July 4 - 6, 2013, Tiruchengode, India.

[9] Qadri, Fleury, M., Altaf, M.,Rofoee, B.R. and Ghanbari, M., ―Resilient P2P multimedia exchange in a VANET‖, 978-1-4244-5661-1.

[10] Mohamed Amine Ferrag and Ahmed Ahmim, "ESSPR: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network", Department of Computer Science, Guelma University and Department of Mathematics and Computer Science, SPRINGER Telecommun Syst 66:481–503, 2017.

[11] Asim Rasheed, Saira Gillani, Sana Ajmal and Amir Qayyum, "Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications", Springer Nature Singapore Pte Ltd. 2017, A. Laouiti et al. (eds.), Vehicular Ad-Hoc Networks for Smart Cities, Advances in Intelligent Systems and Computing 548.

[12] Sunilkumar S. Manvi and Shrikant Tangade, "A survey on authentication schemes in VANETs for secured communication", ELSEVIER Veh. Commun. (2017).

[13] E.Thambiraja, Dr. R.Umarani, G.Ramesh," A Survey of the Elliptic Curve Integrated Encryption Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.

[14] A.Naveena1 and Dr.K.Ramalinga Reddy, "A Review: Elliptical Curve Cryptography in Wireless Ad-hoc Networks", ETM Dept, G.Narayanamma institute of Engineering and Technology for Women. International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 06, June-2016.